Securing Your Home PC

Steps in protecting your home for $100.00

By Frank Simorjay

Lock the door!

- A time ago most people did not lock doors
- The Internet is analogous to the door

- Today we buy locks, and use them
  - A good lock will run you under $100.00
  - Securing your PC can be the same!

- Welcome to the Information superhighway
- *Where your computer is the best kept secret!*

The Risks

- Trojan’s, Viruses,Worms
  - Zombie
  - Use of resources
  - Tunneling
  - theft
- Extortion
- Invasion of Privacy
- Identity Theft
- Disk Crash (not really a security risk)

Virus/Trojans/Worms

- Virus
  - Distributed via e-mail
  - PtoP
  - Chat
  - Website (eg. ActiveX, Java, other scripts)
- Most attacks are not human, but autoRouters (worms).
  - Def: autoRouter a program written to exploit your PC using attacks that are easy to execute. Once successful the program will start to scan for a new victim.
  - Once compromised they can
    - call home
    - capture keystrokes
    - dig for info (find *.dat, *.doc, *.bak, money.*)
    - format HDD
    - replace files (Change AV files).
    - And more!
    - Make you a Zombie (Tunnel server)
    - File storage (FTP host, BitTorrent)
    - Router

The real threats

- Less well known, much more insidious
  - Extortion
  - Invasion of Privacy
  - Identity Theft

Do I really care?

- YES you do!
- The odds are high that you will suffer, if you fail to pay attention to securing your computer.
- The more you wait the worse it can get!
  - Computers are compromised via (number of sources)

–Savvy user, with 4 users in household.

–New DLS service, all users sharing an account.

–In under 2 months.

- *System had over 10 worms, (Sasser, Codered, etc.) 500 spyware related events.*
- *System is unstable, and unusable since one worm locked keyboard from local access. (this was the tip off)*

–Solution:

–Seeked my help, however damage was too extensive to repair.

– ended in rebuild of system (18 hours of work)

- *lock family members out of Admin. Privileges.***

What you need

- If you forget everything from this presentation.
- All you really need to remember is this slide!!!!!
  - Personal Firewall (rec. Zone alarm ~$50.00)
  - AV product (rec. Symantec/Norton ~$50.00)
  - Spam Guard (req. Spamnet ~$0)
  - Popupblocker (Googlebar $0)
  - Spyware watcher (Spybot ~$0-$30)
  - Updates (Microsoft $0!)
  - Phishing protection (Spoofstick $0)
  - Adblocking (Adware $0)
  - ActiveX agent blocker (Spyware Blaster $0)
- Links will be provided in the presentation.

More About security

Other things to think about

ID theft by the numbers

- The single more popular crime of today
- Over 9.9 Million thefts occurred this past year.
- Over 27.3 million thefts over the past 5 years.
  - Why such a growth in this?
  - New mastery in computers (students)
  - Easy, Fast, Difficult to prove, Good return.
    - Some reports of thefts exceeding Millions!
- YOU ARE A GOOD TARGET!
- Source http://www.bankersonline.com/idtheft/mbg_idtheftrealnumbers.html

How to steal an ID

- Collection
  - Collect Name (First Last, Middle)
  - Collect Home Address (Mail zip)
  - Discover Employer
  - Find SSN, DOB
- Search public utilities, banks, court for info.
- Dumpster diving, trash digging.
- Pay for credit check, lots of info.
- http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

I applied for a loan in November 2000 and was told I had bad credit.

I requested a credit report in November 2000 and found all sorts of crazy information on it.

I'm single but was listed as married. When I renewed my driver's license by mail,

I was surprised to find someone else's face on my license.

This is a nightmare and requires a large amount of my time.

From a consumer complaint to the FTC, October 5, 2001

Abuse/Extortion/Invasion of privacy

- New anti-bully laws protect children in school. Bullies have founds ways around it by invading your HOME!
  - Mail, PtoP, Chat (Abusive messaging)
- Pedophiles have found a new means to find targets.
  - Chat (And SIMS are a chat program) (eg. SIMS have a RedLight District)
- Extortion (Do you store ANYTING that could be incriminating on your PC?, Diary, company documents,etc…)
- A tunneled computer can act as a relay.
  - You now are a Porn site web server!
  - Since when do you threaten the president?
  - Why are you advertising cheap meds online?
  - RIAA takes music sharing in-mass very poorly!

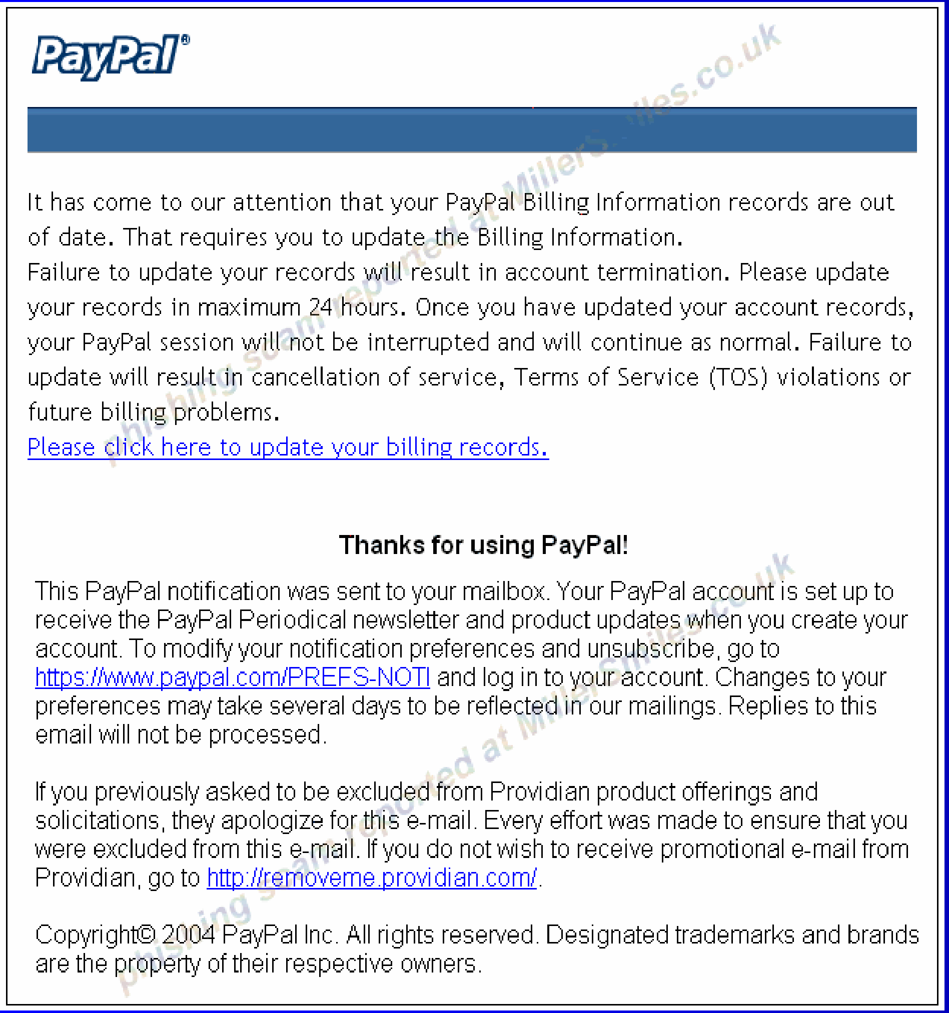
Scams

- Some scammers are becoming savvy.
- Know when your being scammed.
  - First off when it looks too good to be true
    - IT IS!
  - Do not download free software unless it is certified, or has been scrutinized by a community.
  - If you see the need for a free tool, secure your computer first, defend against Virus, Trojans, worms, etc.
  - Protect yourself from redirected websites. Avoid the Click here for more link.
  - And you will never be removed from a mailing list by clicking the ‘click here to be removed from this list’.

Phishing

- More scams. (social engineering)
  - E-mail message from your bank informing you that your account has been compromised, click the link provided to fix the problem. (Note that these message will often have your banks official looking log-in page, and valid return address, However the verification submit link is a keycapture system.)
    - DON’T acknowledge the mail/web page it’s a scam
  - E-mail message from paypal or ebay indicates that your account is about to be deactivated. Unless you click the link to ensure you’re an active user.
    - DON’T acknowledge the mail/web page it’s a scam

Phishing Paypal/AOL



PayPal

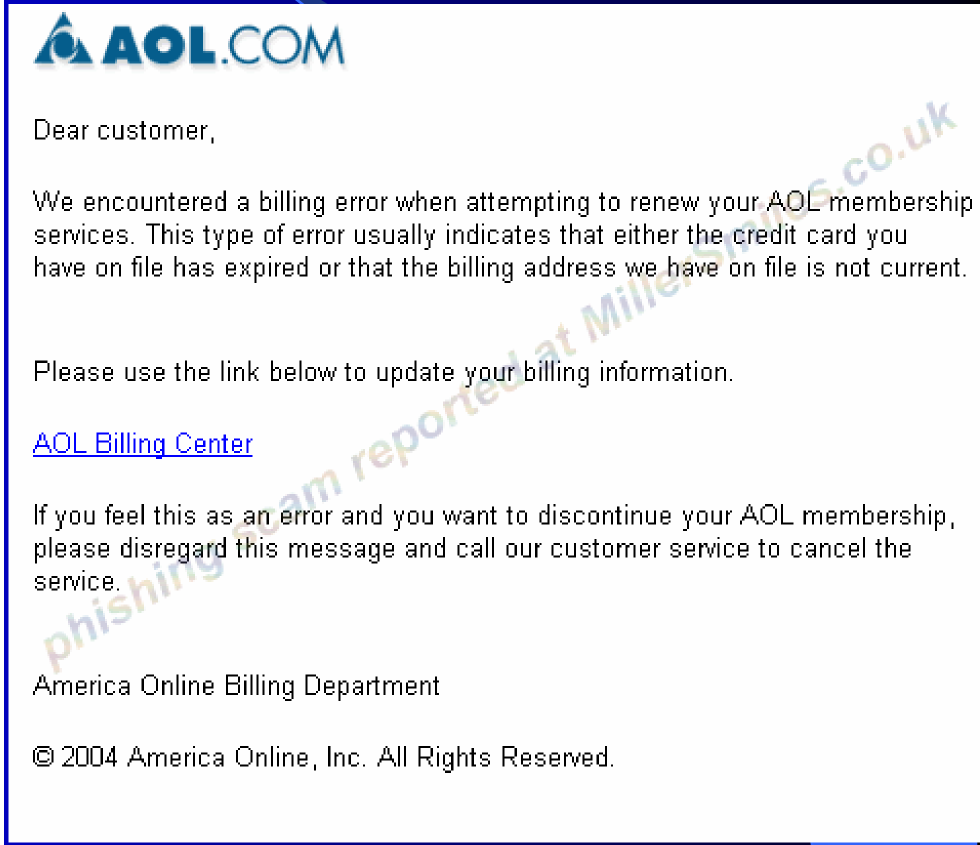
It has come to our attention that your PayPal Billing Information records are out of date. That requires you to update the Billing Information.
Failure to update your records will result in account termination. Please update your records in maximum 24 hours. Once you have updated your account records, your PayPal session will not be interrupted and will continue as normal. Failure to update will result in cancellation of service, Terms of Service (TOS) violations or future billing problems.
Please click here to update your billing records.

Thanks for using PayPal!

This PayPal notification was sent to your mailbox. Your PayPal account is set up to receive the PayPal Periodical newsletter and product updates when you create your account. To modify your notification preferences and unsubscribe, go to https://www.paypal.com/PREFS-NOTI and log in to your account. Changes to your preferences may take several days to be reflected in our mailings. Replies to this email will not be processed.

If you previously asked to be excluded from Providian product offerings and solicitations, they apologize for this e-mail. Every effort was made to ensure that you were excluded from this e-mail. If you do not wish to receive promotional e-mail from Providian, go to http://removeme.providian.com/.

Copyright© 2004 PayPal Inc. All rights reserved. Designated trademarks and brands are the property of their respective owners.



AOL.COM

Dear customer,

We encountered a billing error when attempting to renew your AOL membership services. This type of error usually indicates that either the credit card you have on file has expired or that the billing address we have on file is not current.

Please use the link below to update your billing information.

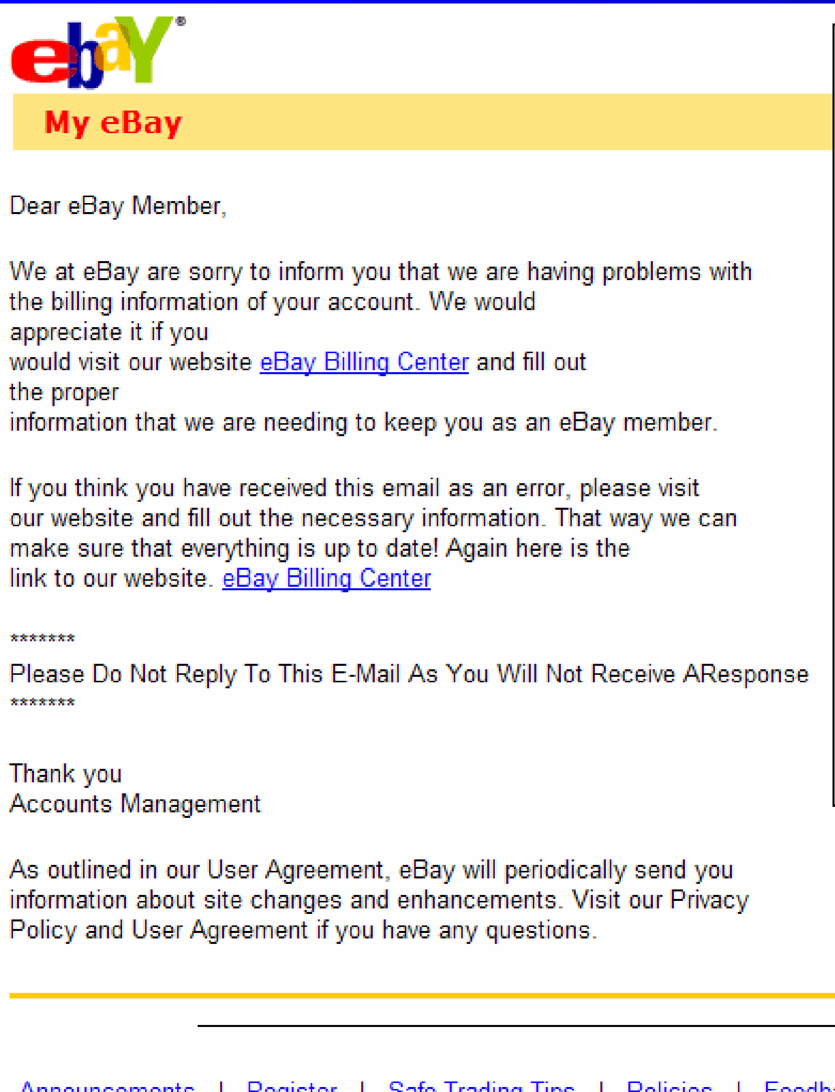
AOL Billing Center

If you feel this as an error and you want to discontinue your AOL membership, please disregard this message and call our customer service to cancel the service.

America Online Billing Department

© 2004 America Online, Inc. All Rights Reserved.

Ebay/USbank



Dear eBay Member,

We at eBay are sorry to inform you that we are having problems with the billing information of your account. We would appreciate it if you would visit our website eBay Billing Center and fill out the proper information that we are needing to keep you as an eBay member.

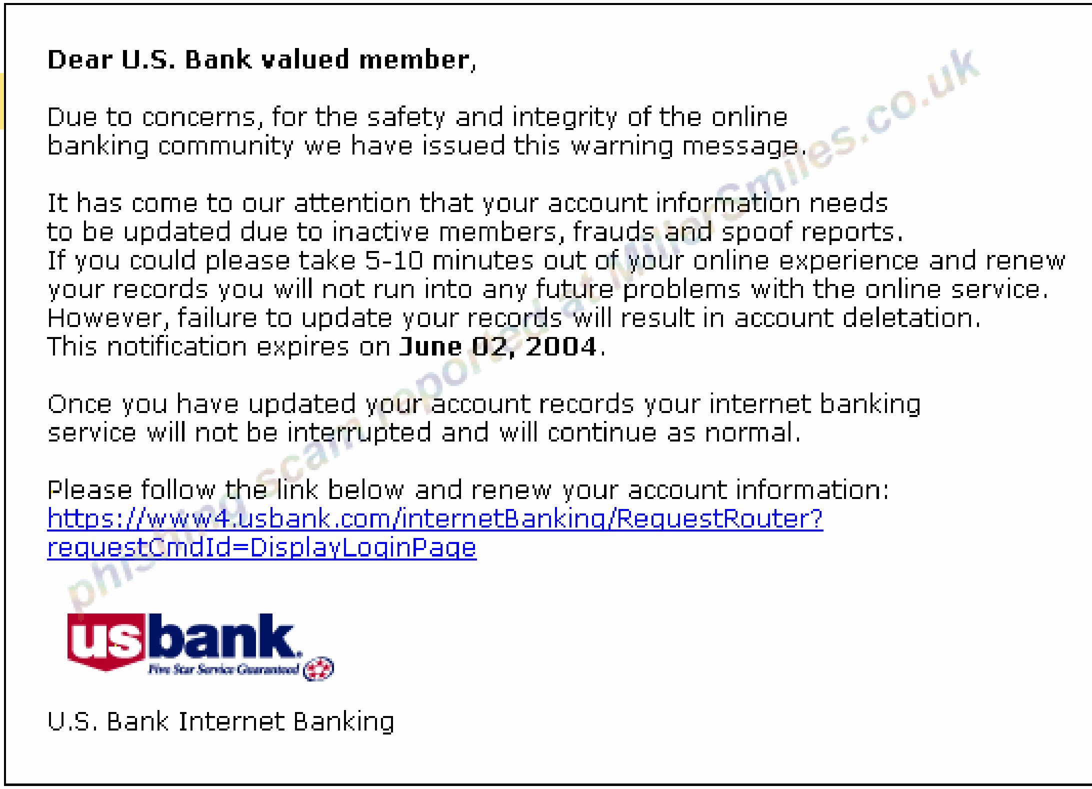
If you think you have received this email as an error, please visit our website and fill out the necessary information. That way we can make sure that everything is up to date! Again here is the link to our website. eBay Billing Center

****
Please Do Not Reply To This E-Mail As You Will Not Receive AResponse
****

Thank you
Accounts Management

As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

Announcements | Register | Safe Trading Tips | Policies | Feedback Forum | About eBay



Dear U.S. Bank valued member,

Due to concerns, for the safety and integrity of the online banking community we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports.
If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service.
However, failure to update your records will result in account deletation.
This notification expires on **June 02, 2004**.

Once you have updated your account records your internet banking service will not be interrupted and will continue as normal.

Please follow the link below and renew your account information:
https://www4.usbank.com/internetBanking/RequestRouter?requestCmdId=DisplayLoginPage

U.S. Bank Internet Banking

Phishing protection

- Two ‘free’ tools are available
- Both ‘flag’ the web site you are visiting
  - If you visit ebay, but are redirected the tools display this information very predominantly.
- Spoofstick can be found at www.corestreet.com/spoofstick (recommended)
- Scamblocker by earthlink can be found at earthlinks website.
- Ebay is has also provided an tool to protect users called Account Guard

Scams

- Additional scams use blank e-mail messages.
- when viewed as HTML, a background browser event will launch.
- This event will capture your key strokes, or upload a Trojan to your computer.
  - This is the primary reason to disable mail views ability to view HTML documents.

Hoaxes

- Fake Trojans/Worms/Virus
  - If you are reading this e-mail you have been infected by FOO??? And can only repair your infection by deleting the following file……kernel.dll…..
- Go to your AV companies web site, most have virus search features, these will often confirm the Hoax.
- Chain letters (plea's for compassion)
  - My son is ill if you send this message to two friends your sprit will help him. Or send 1 dollar to a PO box.
  - A Financial advisor from some African country will pay you a ransom if you open a bank account to deposit his loot.
  - Bill Gates send a message to users to forward a message that will beta test a program. If you forward the message, you be paid Millions!
- More can be found at http://hoaxbusters.ciac.org/

Picking an ISP

- You have a few choices.
- Read up on your soon to be provider. (or existing)
- Don’t use
  - AOL
  - MSN
- Or any so called ‘free’ network unless you are aware that nothing is for free.

Selecting your OS

Picking your Operating system

- Windows 2000/98/ME
  - Others ARE UNSAFE!
- If your not using XP, I strongly recommend the move to Windows XP.
- Use Mac OS 10.X
  - Know that you NEED to patch it. Mac's can be infected, attacked, as well as windows.
- Use Linux 9.X
  - Know your OS.

Windows 2000

- Updates available:
  - http://www.microsoft.com/windows2000
  - Service Pack 4
  - IE Cumulative patch

Windows ME/98

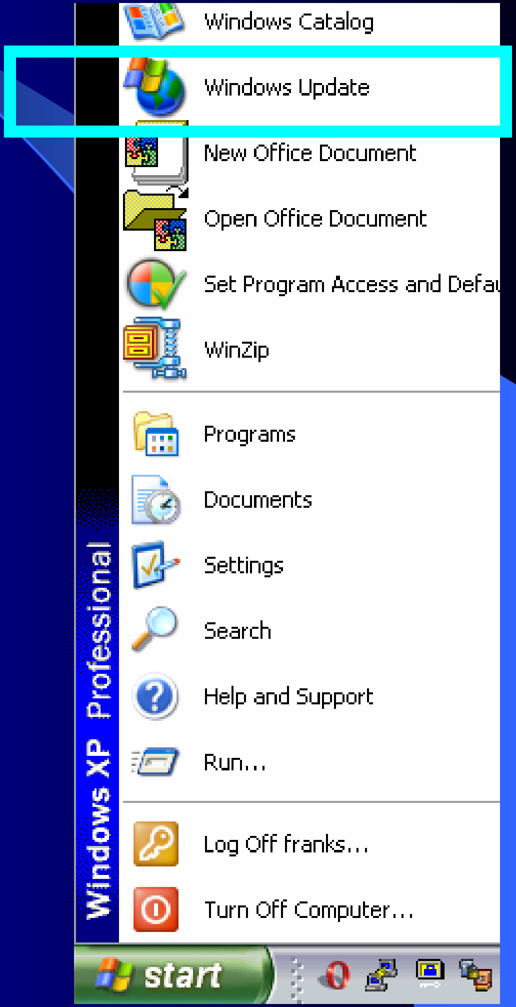
- Difficult to protect, MS recommends a personal firewall!
- Was not built for the internet! And certainly not for security.
- http://www.microsoft.com/windowsME/
- Patch, and maintain, both O/S's require maintenance.

Protection provided by Microsoft

Windows 2000/XP

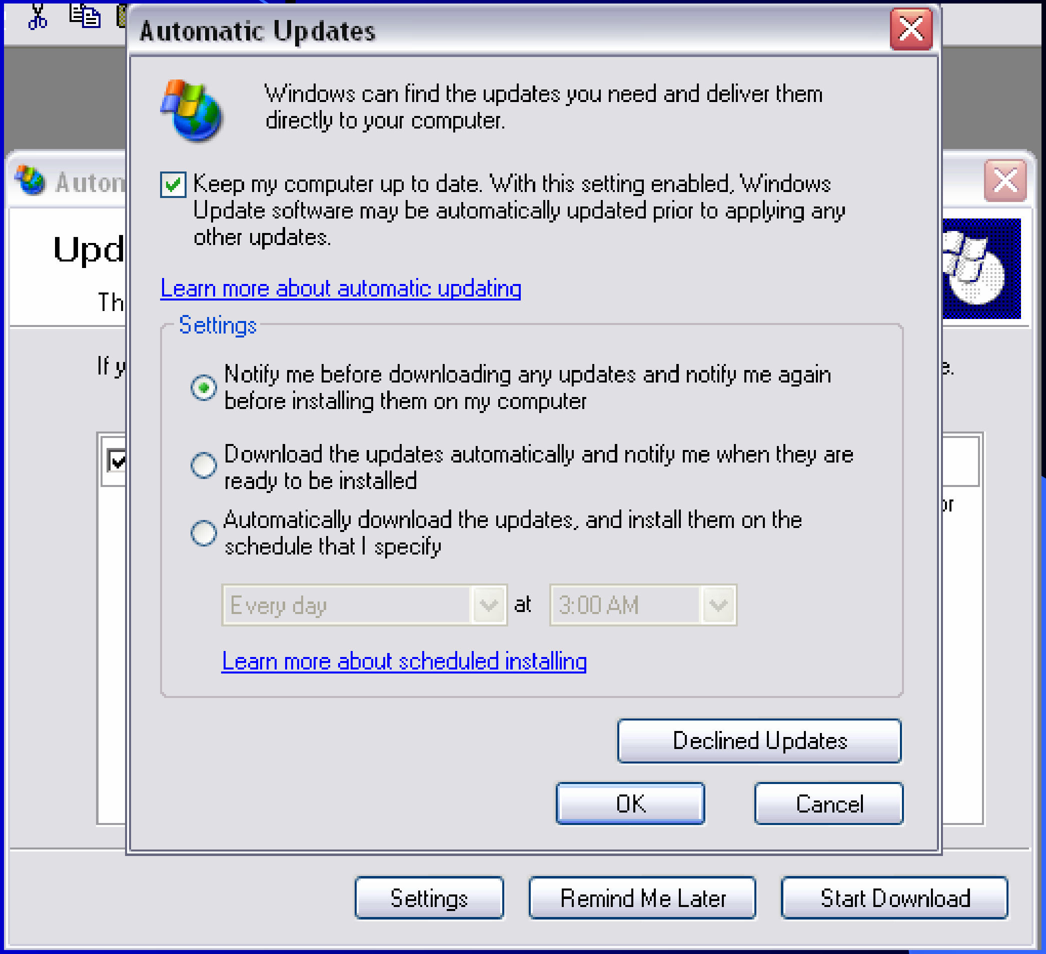
Windows Updates

- Microsoft will have updates for windows XP,2000, and maybe ME
  - XP has updater installed by default.
- Simple to use
  - Most important action to take to protect your computer
  - And it’s FREE!
  - This can also be automated



Automated updates

- Select the window icon from the your taskbar.
- And once the Automated update window comes up, select settings.
- Select Automatically download the updates.



Automatic Updates

Windows can find the updates you need and deliver them directly to your computer.

☑ Keep my computer up to date. With this setting enabled, Windows Update software may be automatically updated prior to applying any other updates.

Learn more about automatic updating

Settings

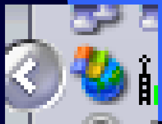
● Notify me before downloading any updates and notify me again before installing them on my computer

○ Download the updates automatically and notify me when they are ready to be installed

○ Automatically download the updates, and install them on the schedule that I specify

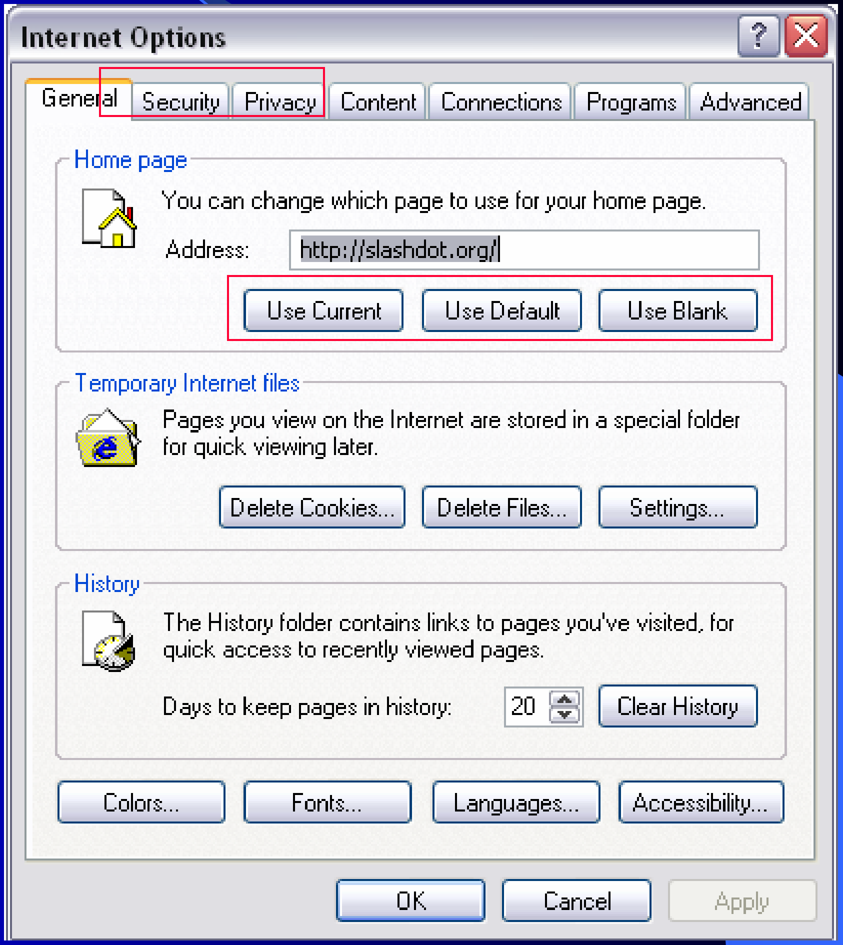
Every day at 3:00 AM

Learn more about scheduled installing



Securing your browser

- A few easy steps.
- In Explorer
  - Select Tools
  - Internet options…



Internet Options

Home page

You can change which page to use for your home page.

Address: http://slashdot.org/

Temporary Internet files

Pages you view on the Internet are stored in a special folder for quick viewing later.

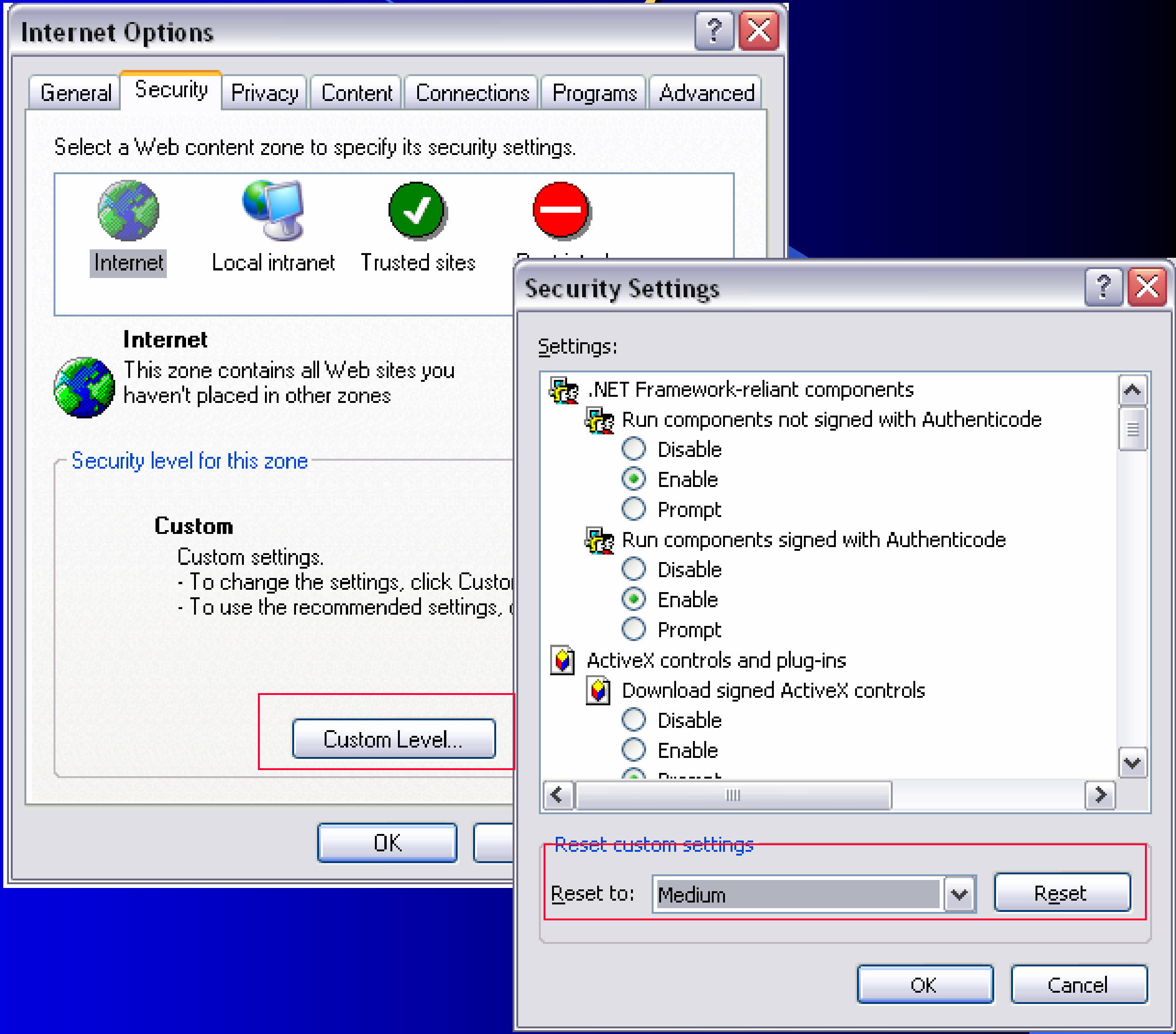
History

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

Days to keep pages in history: 20

Browser security

- In security
- Select
  - Custom level
  - Try High and if this is too restrictive use medium



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a Web content zone to specify its security settings.

Internet | Local intranet | Trusted sites

Internet
This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custo
- To use the recommended settings, c

Custom Level...

OK

Security Settings

Settings:

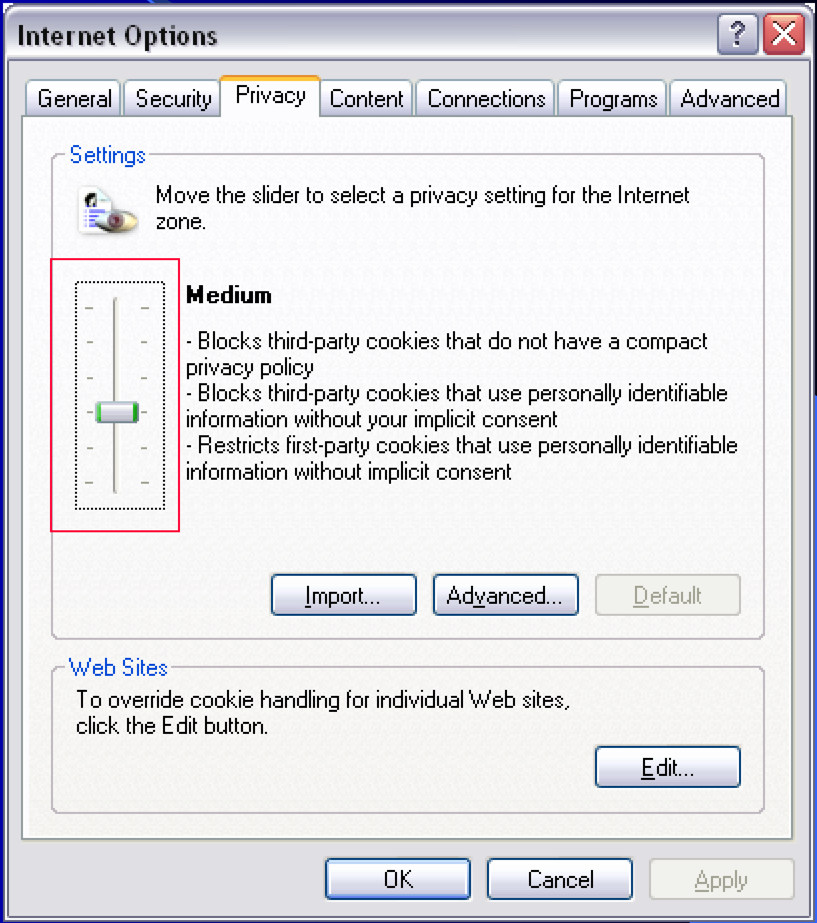
.NET Framework-reliant components
Run components not signed with Authenticode
○ Disable
● Enable
○ Prompt
Run components signed with Authenticode
○ Disable
● Enable
○ Prompt
ActiveX controls and plug-ins
Download signed ActiveX controls
○ Disable
○ Enable
○ Prompt

Reset custom settings
Reset to: Medium
Reset

OK | Cancel

Browser Privacy

- Privacy will reduce the chance that some nasty ID tools are loaded on your system
- Prepare to be confused!
- Choose Medium, or Medium-high.



Internet Options

Settings

Move the slider to select a privacy setting for the Internet zone.

Medium

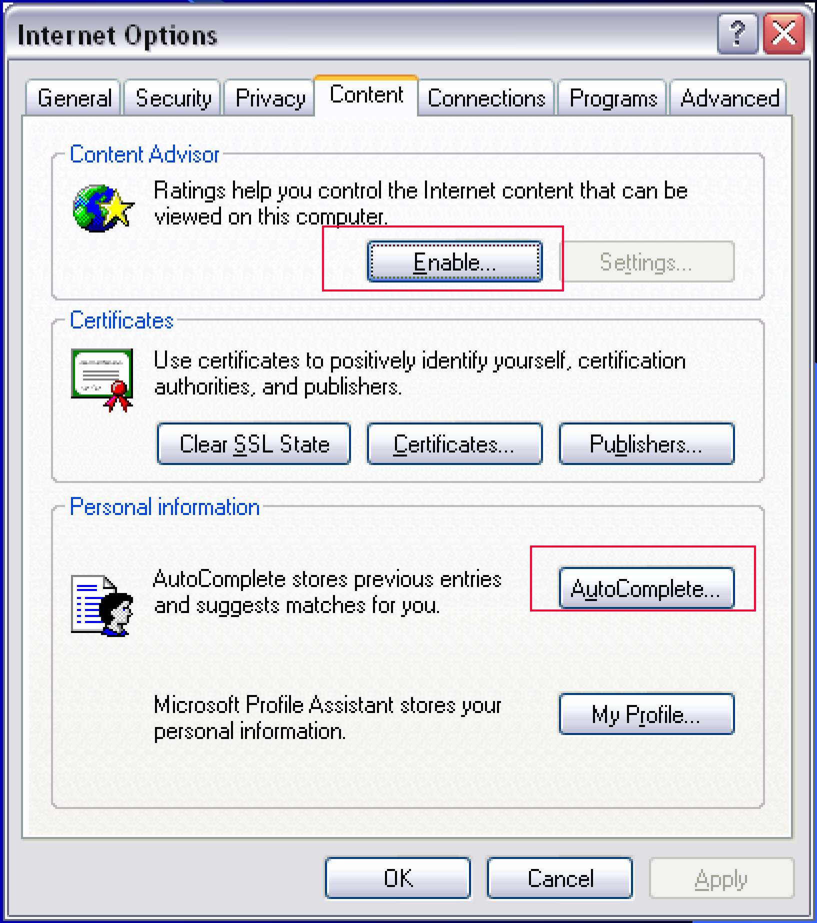
- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Web Sites

To override cookie handling for individual Web sites, click the Edit button.

Content control

- Parents this is worth enabling.
- To enable select enable.
- Also you may want to think about disabling auto complete.



Internet Options

Content Advisor

Ratings help you control the Internet content that can be viewed on this computer.

Certificates

Use certificates to positively identify yourself, certification authorities, and publishers.

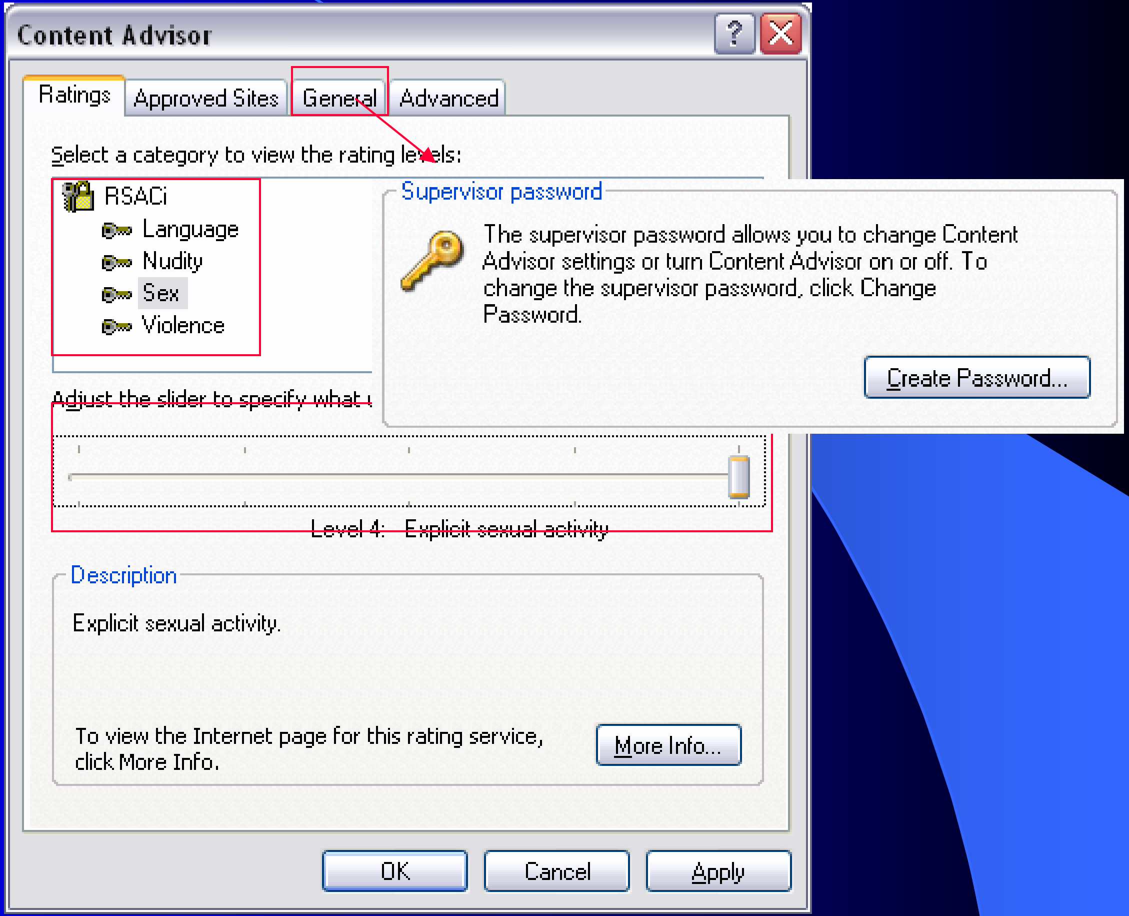
Personal information

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

Configure Content control

- Slide the bar in context window to a acceptable level.
- Make sure to secure your changes with a password
- You can read more about this by clicking ‘More info’



Content Advisor

Select a category to view the rating levels:

Supervisor password

The supervisor password allows you to change Content Advisor settings or turn Content Advisor on or off. To change the supervisor password, click Change Password.

Adjust the slider to specify what

Level 4: Explicit sexual activity

Description

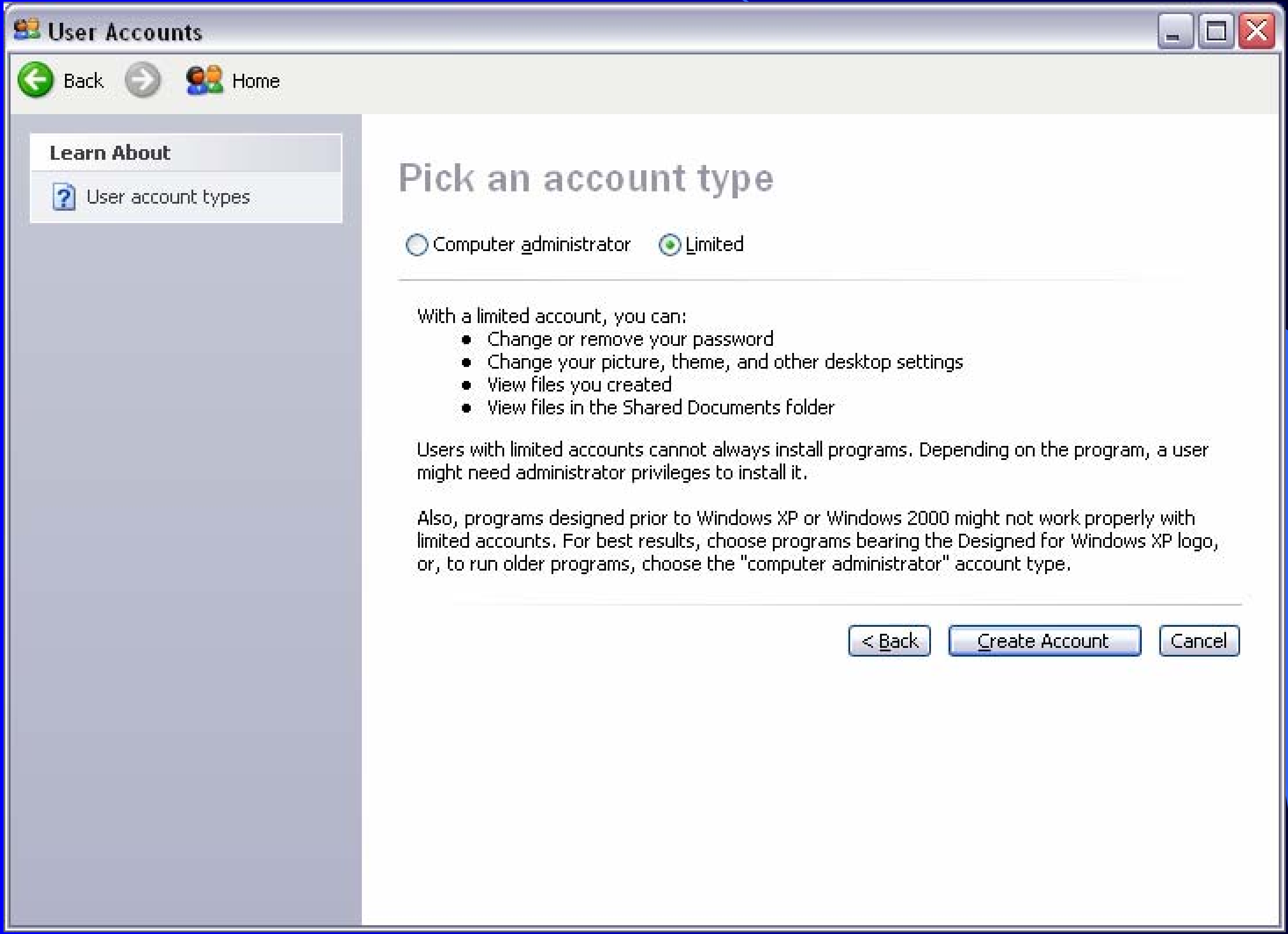
Explicit sexual activity.

To view the Internet page for this rating service, click More Info.

User accounts

- Create user accounts for all family members.
  - -start -> Settings -> Control Panel -> User Accounts -> Create Account
- Prevent family members from Administrative privileges. Make them Limited users.
- Provide a password to the administrator
- CAUTION: These user privileges may effect some programs that do not play well unless all users are administrators.

Limited account



Pick an account type

○ Computer administrator ● Limited

With a limited account, you can:

- Change or remove your password
- Change your picture, theme, and other desktop settings
- View files you created
- View files in the Shared Documents folder

Users with limited accounts cannot always install programs. Depending on the program, a user might need administrator privileges to install it.

Also, programs designed prior to Windows XP or Windows 2000 might not work properly with limited accounts. For best results, choose programs bearing the Designed for Windows XP logo, or, to run older programs, choose the "computer administrator" account type.

3rd party security tools

Some programs (especially spyware does not play well with security tools.)

Personal Firewall

- Several solutions available.
- This will protect information from leaking out, and keep bad programs out.
- Most tools will have intelligent prompts, just follow them.
- Make sure to find out how to key this tool up to date, most have an automated update feature worth enabling.
- Annoyance note: When updating (or patching) alerts may be generated by you Personal Firewall

Personal Firewalls

	Control	Ease of Use	Privacy	Overall	Website
ZoneAlarm Pro	🟩	🟩	🟩	🟩	www.zonelabs.com
Sygate Firewall Pro	🟩	🟩	🟥	🟨	http://www.uant.net/firewall
Norton Firewall	🟩	🟩	🟩	🟩	www.norton.com
McAfee Firewall Plus	🟨	🟨	🟩	🟨	www.McAfee.com
Tiny Personal Firewall	🟥	🟥	🟥	🟥	www.tinysoftware.com

Info custody of http://www.smartcomparisons.com

AV product

- Will protect you from most common Viruses.
- Easy to install, and update.

Make sure to find out how to key this tool up to date, most have an automated update feature worth enabling.

Anti-virus

	Includes Personal Firewall	Includes Popup Blocker	Price / Value	Overall	Website
PC Security Shield	🟩	🟩	🟩	🟩	www.pcsecurityshield.com
McAfee VirusScan	🟩	🟩	🟨	🟩	www.mcafee.com
Titanium AntiVirus	🟨	🟨	🟨	🟨	www.pandasoftware.com
Pc-cillin Net Security	🟨	🟨	🟩	🟨	www.trendmicro.com
Norton AntiVirus	🟩	🟩	🟨	🟨	www.symantec.com
WinAntiVirus	🟨	🟨	🟨	🟨	www.winantivirus.com
AVG AntiVirus	🟨	🟨	🟩	🟨	www.grisoft.com
Protector Plus	🟨	🟨	🟩	🟨	www.pspl.com
NOD32	🟨	🟨	🟨	🟨	www.nod32.com.au

Info custody of http://www.smartcomparisons.com

Spam Guard

- Protects you from Spam.
- Least effective solution. But better than nothing.
- Most only work with Outlook, Outlook Express.
- Will not work with msn,yahoo,aol-mail, other web based e-mails.
- Some ISP's provide this as part of your service.

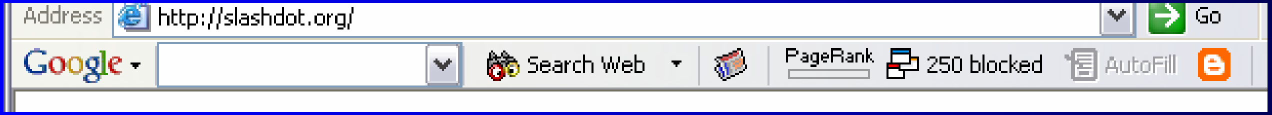
Email / Spam Filters

	Outlook Express Compatibilit	Effectiveness/ Adaptive Technology	Price / Value	Overall	Contact
SpamBully	🟩	🟩	🟩	🟩	www.spambully.com
Qurb	🟨	🟩	🟩	🟩	www.qurb.com
Cloudmark Spamnet	🟨	🟥	🟩	🟨	www.cloudmark.com
McAfee Spamkiller	🟩	🟨	🟨	🟨	www.mcafee.com
iHateSpam	🟨	🟥	🟨	🟨	www.ihatespam.net
MailFrontier Matador	🟨	🟨	🟨	🟨	www.mailfrontier.com
SpamAssassin	🟨	🟨	🟨	🟨	www.spamassassin.org
SurfControl	🟩	🟩	🟥	🟨	www.surfcontrol.com

Info custody of http://www.smartcomparisons.com

Popupblocker

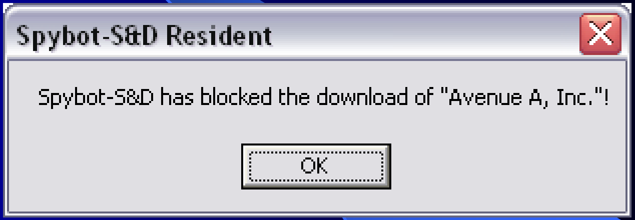
- This will block windows from ‘spawning’ without your consent. (most of the time)
  - Googlebar provided by www.google.com
    - Keyword googlebar
- This will block nasty windows and on the side provide you a nice easy google search interface.



Address http://slashdot.org/

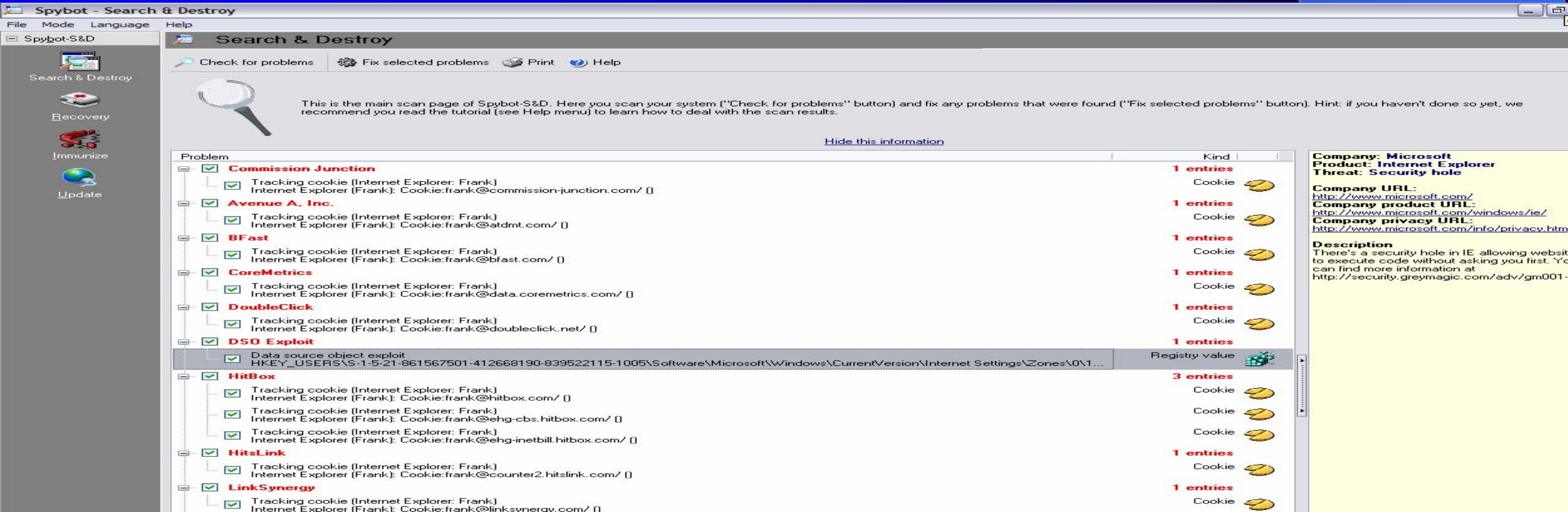
Spyware detector

- This tool provides for a means to remove all foreign spy tools.
- Lots of web sites use spybots/cookies to measure their success, and to track users on site.
    - Additionally some will track you off site
- Spybot, is both easy to use and free
    - http://www.safer-networking.org/



Spybot-S&D Resident

Spybot-S&D has blocked the download of "Avenue A, Inc."!



This is the main scan page of Spybot-S&D. Here you scan your system ("Check for problems" button) and fix any problems that were found ("Fix selected problems" button). Hint: if you haven't done so yet, we recommend you read the tutorial (see Help menu) to learn how to deal with the scan results.

Problem	Kind
☑ **Commission Junction**	**1 entries**
☑ Tracking cookie (Internet Explorer: Frank) Internet Explorer (Frank): Cookie:frank@commission-junction.com/ ()	Cookie
☑ **Avenue A, Inc.**	**1 entries**
☑ Tracking cookie (Internet Explorer: Frank) Internet Explorer (Frank): Cookie:frank@atdmt.com/ ()	Cookie
☑ **BFast**	**1 entries**
☑ Tracking cookie (Internet Explorer: Frank) Internet Explorer (Frank): Cookie:frank@bfast.com/ ()	Cookie
☑ **CoreMetrics**	**1 entries**
☑ Tracking cookie (Internet Explorer: Frank) Internet Explorer (Frank): Cookie:frank@data.coremetrics.com/ ()	Cookie
☑ **DoubleClick**	**1 entries**
☑ Tracking cookie (Internet Explorer: Frank) Internet Explorer (Frank): Cookie:frank@doubleclick.net/ ()	Cookie
☑ **DSO Exploit**	**1 entries**
☑ Data source object exploit HKEY_USERS\S-1-5-21-861567501-412668190-839522115-1005\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1...	Registry value
☑ **HitBox**	**3 entries**
☑ Tracking cookie (Internet Explorer: Frank) Internet Explorer (Frank): Cookie:frank@hitbox.com/ ()	Cookie
☑ Tracking cookie (Internet Explorer: Frank) Internet Explorer (Frank): Cookie:frank@ehg-cbs.hitbox.com/ ()	Cookie
☑ Tracking cookie (Internet Explorer: Frank) Internet Explorer (Frank): Cookie:frank@ehg-inetbill.hitbox.com/ ()	Cookie
☑ **HitsLink**	**1 entries**
☑ Tracking cookie (Internet Explorer: Frank) Internet Explorer (Frank): Cookie:frank@counter2.hitslink.com/ ()	Cookie
☑ **LinkSynergy**	**1 entries**
☑ Tracking cookie (Internet Explorer: Frank) Internet Explorer (Frank): Cookie:frank@linksynergy.com/ ()	Cookie

Company: Microsoft
Product: Internet Explorer
Threat: Security hole

Company URL:
http://www.microsoft.com/
Company product URL:
http://www.microsoft.com/windows/ie/
Company privacy URL:
http://www.microsoft.com/info/privacy.htm

Description
There's a security hole in IE allowing websit
to execute code without asking you first. Yo
can find more information at
http://security.greymagic.com/adv/gm001-

More Spyware

- Adware such as adblocker and etc. are also great add-ons, be aware that they may conflict with the spyware.
- Use with caution.
- www.lavasoftusa.com

Other Desktop protection

- SpywareBlaster
  Doc Scrubber
  MRU-Blaster
  SpywareGuard
  Windows Media Player Scripting Fix
  ID-Blaster Plus
  FileChecker

- www.javacoolsoftware.com

Safe Usage

- Inform family members that mail, chats, etc. are monitored.
- You check logs, and reserve the right to ban a family member (treat it as a CAR + Insurance)
- Sites that require parent guidance, or approval, must go past YOU!.
- More about this in the Bonus section -+-+-+

Be calm don’t panic

- Install programs 1 at a time.
- Read the ‘read me’ documents.
- If you can test temporarily out do. (Zone labs offers to block programs once, or all time. Test it first)
- Try changes as all users.

Safe-r

- The simple steps to secure your computer
  - Personal Firewall (rec. Zone alarm ~$50.00)
  - AV product (rec. Symantec/Norton ~$50.00)
  - Spam Guard (req. Spamnet ~$0)*
  - Popupblocker (Googlebar $0)
  - Spyware watcher (Spybot ~$0-$30)
  - Updates (Microsoft $0!)
- But wait!

Bonus Points

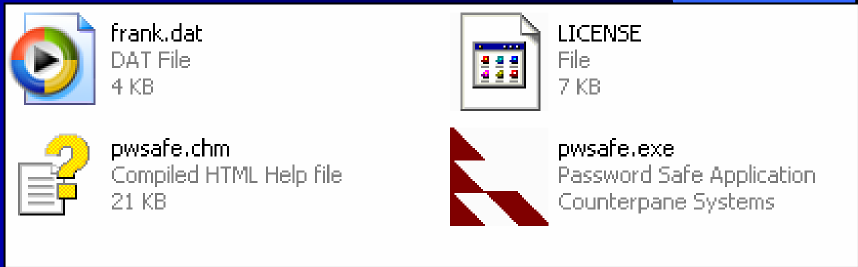
A few more pointers

Passwords

- Keep your passwords complex, no words, mix is best
- Try and changes frequently

BAD	Better
password	12pass34word!
flowers	9flow2er#
money	Mo6ney6$

- Password maintainer.
- Passwordsafe (free)
  - Tip -> a $20 64 MB USB key for storage!
  - Place password safe directory on key, passwords now are portable.
- http://passwordsafe.sourceforge.net



frank.dat
DAT File
4 KB

LICENSE
File
7 KB

pwsafe.chm
Compiled HTML Help file
21 KB

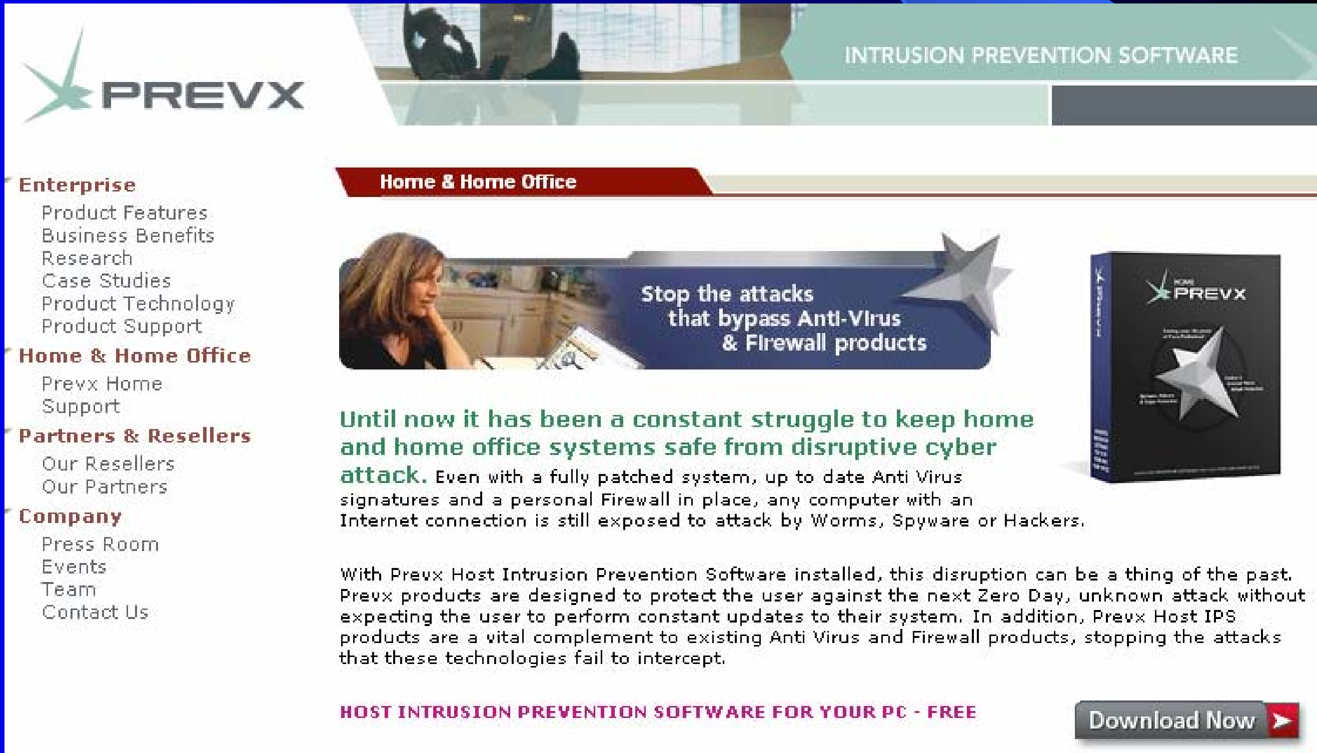
pwsafe.exe
Password Safe Application
Counterpane Systems

Wireless

- Useful, simple, easy to install.
- Be careful, and if you are going to use it check to see who else is using it.
- netstumbler is a free tool that will identify anyone ‘borrowing your wireless’
- Try and place the AP in the center of the house.
- Secure your pc’s!

IPS

- Free tools are good.
- Free IPS will block more bad things. A bit more advanced.
  - DOS
  - DDOS
  - Other new attacks
  - https://www.prevx.com/homeoffice/homeoffice.htm



Until now it has been a constant struggle to keep home and home office systems safe from disruptive cyber attack. Even with a fully patched system, up to date Anti Virus signatures and a personal Firewall in place, any computer with an Internet connection is still exposed to attack by Worms, Spyware or Hackers.

With Prevx Host Intrusion Prevention Software installed, this disruption can be a thing of the past. Prevx products are designed to protect the user against the next Zero Day, unknown attack without expecting the user to perform constant updates to their system. In addition, Prevx Host IPS products are a vital complement to existing Anti Virus and Firewall products, stopping the attacks that these technologies fail to intercept.

HOST INTRUSION PREVENTION SOFTWARE FOR YOUR PC - FREE

Summary

Simple steps to Protect yourself

- Patch
- Protect your passwords
- Lock down your system
- Awareness of scams
- Protect your privacy, and identity
- Be aware of Hoaxes
- Provide Safe Computer Rules to family

Go home be safe.